



# Trend Micro Deep Security

Seguridad del servidor



Protección de los  
centros de datos  
dinámicos

*Artículo técnico  
de Trend Micro | Agosto de 2009*

## I. SEGURIDAD EN EL CENTRO DE DATOS DINÁMICO

El objetivo de la seguridad de TI consiste en permitir las operaciones empresariales, no en obstaculizarlas, pero cada día son más los retos y dificultades a los que se deben hacer frente en relación con este asunto. Los requisitos de cumplimiento imponen una serie de estándares de seguridad para los datos y aplicaciones que residen en los servidores. Los servidores físicos se están sustituyendo por equipos virtuales para ahorrar dinero, ser más ecológicos y aumentar la escalabilidad. La informática en Internet ha hecho evolucionar la infraestructura de TI tradicional para aumentar el ahorro económico y mejorar la flexibilidad, la capacidad y las opciones. Los servidores ya no se encuentran atrincherados tras defensas perimetrales y, como sucediera anteriormente con los equipos portátiles, están traspasando el perímetro de seguridad y necesitan una última línea de defensa. Por lo tanto, ahora en la estrategia de seguridad de defensa exhaustiva es esencial implementar un servidor y un sistema de protección de aplicaciones que proporcione controles de seguridad completos y que, además, sea compatible con los entornos de TI de ahora y de mañana. Trend Micro da respuesta a todos estos desafíos con la solución Deep Security.



### **SERVIDORES BAJO PRESIÓN**

Según el informe *Data Breach Investigations Report* realizado en 2008 por el Risk Team de Verizon Business, el 59% de las filtraciones de datos se produjo a causa de las actividades de hackers e intrusiones. Las filtraciones TJX y Hannaford subrayaron la posibilidad de que los riesgos del sistema influyeran negativamente en la reputación y las operaciones de cualquier negocio de forma significativa. Las organizaciones prosiguen con su lucha por encontrar un equilibrio entre la necesidad de proteger sus recursos y la necesidad de ampliar el acceso a esos mismos recursos a más clientes y socios empresariales.

Los estándares de datos del sector de tarjetas como medio de pago (PCI DSS) actuales reconocen que las defensas perimetrales tradicionales no son suficientes para proteger los datos de las amenazas más recientes y que ahora son necesarias varias capas de protección que van más allá del cortafuegos basado en appliances y los sistemas de detección y prevención de intrusiones (IDS/IPS). Redes inalámbricas, ataques cifrados, recursos móviles, aplicaciones Web vulnerables... todos ellos contribuyen a alimentar los puntos débiles que exponen a los servidores de la empresa a intrusiones y riesgos varios.

En los últimos cinco años, las plataformas informáticas de centro de datos, que durante mucho tiempo se han basado en los servidores físicos, han sufrido un inmenso cambio tecnológico. Así, el impacto de los centros de datos tradicionales se está reduciendo para dar paso a un ahorro de costes y una TI “más verde” gracias a la consolidación de servidores. Casi todas las organizaciones han virtualizado parcial o totalmente las cargas de trabajo del centro de datos, lo cual permite un uso multiempresarial (*multi-tenant*) de lo que antes eran servidores físicos de empresa u objetivo únicos. El grupo Gartner prevé que, de aquí al 2011, la base instalada de equipos virtuales se multiplique por diez y, asimismo, se espera que para el 2012 la mayor parte de la carga de trabajo de los servidores de x86 se ejecute en equipos virtuales.

## **SERVIDORES QUE SE MULTIPLICAN RÁPIDAMENTE Y EN TRÁNSITO**

Las enormes ventajas que la virtualización de TI reporta a las organizaciones son las causantes de que este método se haya adoptado de forma generalizada. La virtualización aumenta las posibilidades y la capacidad de respuesta ante la demanda corporativa, al tiempo que un uso más eficaz de las licencias de hardware y software permite conseguir una consolidación continuada de las cargas de trabajo. En un entorno virtual, la estricta separación entre dispositivos de red y servidores se reduce, por cuanto ahora ambos se combinan en las plataformas de virtualización. Sin embargo, dado que las appliances de seguridad de la red son totalmente ajenas al tráfico que fluye entre los equipos virtuales, el alojamiento de las cargas de trabajo de distintos niveles brinda la oportunidad de llevar a cabo ataques. Las herramientas de tránsito (fundamentales para gestionar el tiempo de inactividad programado, el uso adecuado de los recursos de virtualización y la disponibilidad de las aplicaciones) suponen otra carga de trabajo más para el servidor que tiene un impacto en la gestión del historial de cumplimiento y las appliances de seguridad virtuales. De igual modo, la inevitable “expansión” de los equipos virtuales aumenta las probabilidades de que aquellos que no apliquen los parches más recientes queden expuestos al tráfico malicioso. El personal de TI debe estudiar muy detenidamente los métodos que se usan para proteger las instancias de los servidores empresariales.

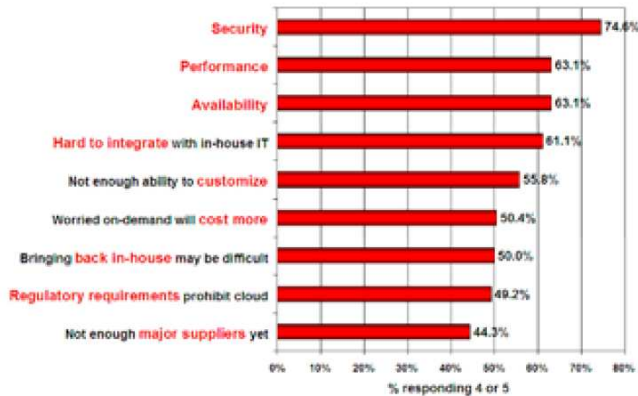
## **SERVICIOS ABIERTOS EN INTERNET**

La informática en Internet amplía la capacidad de una empresa de cubrir la demanda informática en sus operaciones cotidianas. Ante un número cada vez mayor de organizaciones que se decantan por la informática en Internet y la creación de redes públicas por parte de los proveedores de servicio, el modelo de seguridad sigue afrontando el reto de alojar todas estas cargas de trabajo virtualizadas de manera efectiva. La seguridad es el área que genera más indecisión entre las organizaciones a la hora de trasladar las cargas de trabajo de sus negocios a las redes públicas. Recientemente, IDC realizó una encuesta entre 244 directores/ejecutivos de TI y sus colegas de línea de negocios para evaluar sus opiniones y saber el uso que sus compañías hacían de los servicios informáticos de Internet, y la seguridad obtuvo el primer puesto como principal desafío de la informática en Internet.

Cuando un servidor se traslada a los recursos de Internet públicos, el perímetro del centro de datos deja de ser una barrera de protección, ya que los servidores virtualizados proporcionan acceso administrativo directamente desde Internet. La consecuencia de esto es que los problemas que ya existían en el centro de datos (como la gestión de los parches y los informes de cumplimiento), adquieren una magnitud mucho mayor. La única protección significativa en Internet es el denominador común mínimo que el proveedor puede proporcionar en su perímetro, o los mecanismos que una

organización puede aplicar a su equipo virtual para que pueda defenderse por sí mismo, dado que se aloja en servidores junto con las cargas de trabajo de otras organizaciones.

**Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model**  
(1=not significant, 5=very significant)



“La seguridad es, con mucho, el principal problema de los servicios por Internet. Al ver la información y recursos de TI fundamentales de sus negocios fuera de la protección del cortafuegos, los clientes se preocupan ante la posibilidad de sufrir un ataque.”

– Frank Gens, vicepresidente y analista jefe, IDC

## II. TREND MICRO DEEP SECURITY: DESCRIPCIÓN GENERAL

La solución Trend Micro Deep Security es un software de protección de servidores y aplicaciones que unifica la seguridad de los entornos de centros de datos tradicionales, virtuales y en Internet. Ayuda a las organizaciones a evitar que se produzcan filtraciones de datos e interrupciones en la productividad empresarial y a cumplir con las normativas y estándares clave (incluido PCI) y, asimismo, permite reducir el coste de las operaciones necesarias dado el clima económico actual. La solución Deep Security, que permite que los sistemas dispongan de autodefensa, se ha optimizado para proteger los datos confidenciales y garantizar la disponibilidad de las aplicaciones. Esta solución ofrece una protección completa que incluye los siguientes elementos:

- Inspección profunda de paquetes que posibilita la detección y prevención de intrusiones, la protección de aplicaciones Web y el control de aplicaciones
- Cortafuegos de inspección de estado
- Supervisión de integridad del sistema y los archivos
- Inspección de registros

### III. SEGURIDAD COMPLETA Y FÁCIL DE GESTIONAR

La solución Deep Security se vale de módulos para cumplir con los requisitos imprescindibles de protección de aplicaciones y servidores:

Requisito del centro de datos	Módulos de Deep Security					
	Inspección profunda de paquetes			Corta-fuegos	Supervisión de integridad	Inspección de registros
	IDS/IPS	Protección de aplicaciones Web	Control de aplicaciones			
<b>Protección de servidores</b> <ul style="list-style-type: none"> <li>Protege contra los ataques conocidos y de día cero</li> <li>Ofrece una defensa de las vulnerabilidades hasta que se apliquen los parches necesarios</li> </ul>	●			●	●	○
<b>Protección de aplicaciones Web</b> <ul style="list-style-type: none"> <li>Protección frente a ataques por Internet como SQL Injection, secuencias de sitios cruzados y ataques por la fuerza bruta</li> <li>Cumple el requisito 6.5 de PCI DSS (cortafuegos de aplicaciones Web)</li> </ul>	●	●			○	●
<b>Seguridad de virtualización</b> <ul style="list-style-type: none"> <li>Protege contra los ataques conocidos y de día cero</li> <li>Ofrece una defensa de las vulnerabilidades hasta que se apliquen los parches necesarios</li> <li>La integración de VMware vCenter mejora la visibilidad y la gestión</li> </ul>	●	○		●	●	○
<b>Detección de comportamiento sospechoso</b> <ul style="list-style-type: none"> <li>Protección frente a las exploraciones de reconocimiento</li> <li>Detección de protocolos permitidos en puertos inadecuados</li> <li>Alerta sobre errores de sistema operativo y aplicaciones que podrían ser indicativos de un ataque</li> <li>Alerta sobre cambios en las aplicaciones o sistema operativo críticos</li> </ul>	○		●	●	●	●
<b>Seguridad de informática en Internet</b> <ul style="list-style-type: none"> <li>Uso de políticas de cortafuegos para aislar los equipos virtuales</li> <li>Protege contra los ataques conocidos y de día cero</li> <li>Ofrece una defensa de las vulnerabilidades hasta que se apliquen los parches necesarios</li> </ul>	●	○		●	●	●
<b>Informes sobre el cumplimiento de normativas</b> <ul style="list-style-type: none"> <li>Visibilidad y registro de auditorías de todos los cambios que tienen lugar en los servidores críticos</li> <li>Inspección, correlación y reenvío de los eventos de seguridad importantes a los servidores de registro para tareas de protección, documentación y archivado</li> <li>Informes sobre configuraciones y detección e interrupción de actividades</li> </ul>	○	●	○	○	●	●

● = Esencial ○ = Ventajoso

### IV. VENTAJAS

Las arquitecturas de seguridad de los servidores de un centro de datos deben asimilar los cambios que tienen lugar en las arquitecturas de TI, como la virtualización y consolidación, los nuevos modelos de suministro del servicio y la informática en Internet. En este sentido, las soluciones Deep Security ayudan a que todos los modelos de centro de datos puedan realizar las siguientes tareas:

- Evitar las filtraciones de datos y las interrupciones en la productividad empresarial al:
  - Ofrecer una línea de defensa en el propio servidor, ya sea físico, virtual o en Internet
  - Proteger las vulnerabilidades (conocidas y no conocidas) de las aplicaciones Web y empresariales y de los sistemas operativos, además de bloquear los ataques dirigidos a estos sistemas
  - Fomentar la identificación de actividades y comportamientos sospechosos y tomar medidas proactivas y preventivas

- Permitir el cumplimiento al:
  - Satisfacer seis de los principales requisitos de cumplimiento de PCI (como la seguridad de las aplicaciones Web, la supervisión de la integridad de los archivos y la recopilación de registros de servidor), junto con otros muchos requisitos para el cumplimiento de normativas
  - Proporcionar informes detallados de auditoría que describen los ataques que se han evitado y el estado de cumplimiento de las políticas, lo cual reduce el tiempo de preparación necesario para realizar las auditorías
- Disminuir los costes operativos al:
  - Ofrecer protección de las vulnerabilidades a fin de dar prioridad a los esfuerzos de codificación segura y de poder implementar los parches no programados de forma más rentable
  - Proporcionar la seguridad que las organizaciones necesitan para aprovechar al máximo la virtualización o la informática en Internet y materializar las reducciones de costes intrínsecas de estos enfoques
  - Ofrecer una protección completa en un solo agente de software gestionado centralizadamente, de modo que se pone fin a la necesidad de implementar varios clientes de software (y a los costes derivados de ello)

## V. MÓDULOS Y FUNCIONALIDAD

La solución Deep Security permite implementar uno o varios módulos de protección dedicando únicamente el nivel de protección adecuado para cumplir los requisitos empresariales particulares en continuo cambio. Así, puede optar por crear servidores y equipos virtuales con autodefensa mediante la implementación de una protección completa, o bien por empezar con el módulo de supervisión de la integridad para destapar cualquier comportamiento sospechoso. Todas las funciones modulares se implementan en el servidor o el equipo virtual a través de un solo Deep Security Agent, que el software de Deep Security Manager gestiona de forma centralizada y unifica en todos los entornos, sean éstos físicos, virtuales o en Internet.

### ***MOTOR DE INSPECCIÓN PROFUNDA DE PAQUETES (DPI)***

#### ***Activación de la detección y prevención de intrusiones, la protección de aplicaciones Web y el control de aplicaciones***

Con el motor de elevado rendimiento para la inspección profunda de paquetes de la solución se supervisa el tráfico entrante y saliente, incluido el tráfico SSL, en busca de desviaciones del protocolo de red, contenido sospechoso que indique un ataque e infracciones de las políticas de seguridad. Este motor puede funcionar en el modo de detección y prevención para proteger los sistemas operativos y las vulnerabilidades de las aplicaciones empresariales. Protege las aplicaciones Web de los ataques a la capa de aplicación, incluidos SQL Injection y secuencias de sitios cruzados. Los eventos pormenorizados ofrecen información valiosa, que indica quién atacó, cuándo se produjo el ataque y qué vulnerabilidad se intentó aprovechar. Los administradores reciben notificaciones automáticas mediante alertas cuando se ha producido un incidente. DPI se usa en las tareas de detección y prevención de intrusiones, protección de aplicaciones Web y control de aplicaciones.

## **SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)**

### ***Protección de las vulnerabilidades de los sistemas operativos y las aplicaciones empresariales hasta que se les puedan aplicar parches para obtener la protección oportuna frente a los ataques conocidos y de día cero***

Las reglas de vulnerabilidad protegen las vulnerabilidades conocidas (por ejemplo, aquellas que se revelan en 'Microsoft Tuesday'), de una serie ilimitada de explotaciones. La solución Deep Security incluye protección inmediata de vulnerabilidades para más de 100 aplicaciones, incluidas bases de datos, sitios Web, correo electrónico y servidores FTP. Las reglas que protegen las nuevas vulnerabilidades descubiertas se entregan automáticamente al cabo de pocas horas y se pueden enviar a miles de servidores en cuestión de minutos, sin necesidad de reiniciar el sistema.

- Las reglas inteligentes ofrecen protección de día cero frente a ataques no conocidos que pueden aprovechar las vulnerabilidades no conocidas mediante la detección de datos de protocolo no usuales que contienen código malicioso.
- Las reglas de explotación detienen los ataques y malware conocidos y se parecen a los softwares antivirus tradicionales por el hecho de utilizar firmas para identificar y bloquear las explotaciones individuales conocidas.

Al ser miembro "inaugural" del programa Microsoft Active Protections Program (MAPP), la solución Deep Security recibe información sobre vulnerabilidades procedente de Microsoft por adelantado, a través de sus boletines de seguridad mensuales. Estos avisos con antelación permiten anticiparse a las amenazas emergentes, así como proveer a los clientes comunes de protecciones más oportunas con total eficacia mediante actualizaciones de seguridad.

## **SEGURIDAD DE LAS APLICACIONES WEB**

La solución Deep Security permite cumplir el requisito 6.6 de PCI relativo a la protección de las aplicaciones Web y los datos que éstas procesan. Las reglas de protección de aplicaciones Web proporcionan una defensa frente a los ataques SQL Injection, secuencias de sitios cruzados y otras vulnerabilidades de aplicaciones Web, y protegen estas vulnerabilidades hasta que se realizan las correcciones de código pertinentes. La solución emplea reglas inteligentes para identificar y bloquear los ataques de aplicaciones Web más habituales. Un centro de datos de SaaS en el que se ha implementado Deep Security fue capaz de proteger el 99% de todas las vulnerabilidades más importantes detectadas en sus servidores y aplicaciones Web por medio de un test de penetración solicitado por los clientes.

## **CONTROL DE APLICACIONES**

Las reglas de control de aplicaciones permiten una mayor visibilidad o control de las aplicaciones que tienen acceso a la red. Estas reglas también pueden servir para identificar el software malicioso que tiene acceso a la red y para disminuir la vulnerabilidad de los servidores.

## CORTAFUEGOS

### **Disminución de la superficie de ataque de los servidores físicos y virtuales**

El módulo de software de cortafuegos de Deep Security, que está pensado para empresas, es bidireccional y dispone de inspección del estado. Sirve para permitir las comunicaciones a través de los puertos y protocolos necesarios para corregir el funcionamiento del servidor y, asimismo, para bloquear el resto de puertos y protocolos, con lo cual se reduce el riesgo de que se produzca un acceso no autorizado al servidor. Entre sus características se incluyen:

- Aislamiento de los equipos virtuales: permite el aislamiento de los equipos virtuales en entornos virtuales multiempresariales (*multi-tenant*) o de informática en Internet, lo cual proporciona una segmentación virtual sin necesidad de modificar las configuraciones de los conmutadores virtuales.
- Filtrado avanzado: el tráfico se filtra mediante reglas de cortafuegos basadas en direcciones IP, direcciones Mac, puertos, etc. Se pueden configurar distintas políticas para cada interfaz de la red.
- Cobertura de todos los protocolos basados en IP: la posibilidad de capturar paquetes completos simplifica las tareas de solución de problemas y proporciona una información muy valiosa para poder entender los eventos de cortafuegos que surgen (TCP, UDP, ICMP, etc.).
- Detección de exploraciones: detecta actividades como la exploración de puertos. El tráfico que no es de IP, como el tráfico ARP, también se puede restringir.
- Control flexible: el firewall de inspección de estado es flexible, por lo que permite omitir completamente la inspección de manera controlada cuando sea necesario. Trata las características de tráfico ambiguas que se pueden hallar en cualquier red, ya sea debido a condiciones normales o como parte de un ataque.
- Perfiles de cortafuegos predefinidos: se establecen grupos de tipos comunes de servidor empresarial (como, por ejemplo, Web, LDAP, DHCP, FTP y de base de datos), lo cual garantiza una implementación rápida, sencilla y coherente de la política de cortafuegos, incluso en redes grandes y complejas.
- Informes que permiten acciones: gracias a los registros detallados, las alertas, los paneles y la generación de informes flexibles, el módulo de cortafuegos de Deep Security captura los cambios de configuración (como los cambios de política que se han efectuado y quién los ha efectuado) y realiza un seguimiento de los mismos, de modo que se obtiene un registro de auditoría realmente pormenorizado.

## SUPERVISIÓN DE INTEGRIDAD

### **Supervisión de cambios sospechosos, imprevistos o no autorizados**

El módulo de software de supervisión de la integridad de Deep Security supervisa los archivos del sistema operativo y de aplicaciones básicos (directorios, claves de registro, valores, etc.) para detectar cambios maliciosos e inesperados. Entre sus características se incluyen:

- Detección bajo petición o programada: las exploraciones de integridad se pueden programar o realizar según la demanda.
- Comprobación extensiva de las propiedades de archivo: los archivos y directorios se pueden supervisar para detectar cualquier cambio realizado en elementos como el contenido, los atributos (como los propietarios, los permisos y el tamaño) y la marca de fecha y hora, todo ello a través de reglas de integridad de uso inmediato. Las adiciones, modificaciones o eliminaciones de las claves y valores del registro, las listas de control de acceso y los archivos de registro también se pueden supervisar e informar al respecto. Esta función es aplicable al requisito 10.5.5 de PCI DSS.

- Informes de auditoría: el módulo de supervisión de la integración puede mostrar eventos de integridad en el panel de Deep Security Manager, así como generar alertas e informes fáciles de auditar. De igual modo, puede reenviar eventos a un sistema de gestión de información de seguridad y eventos (SIEM) a través de Syslog.
- Grupos de perfiles de seguridad: las reglas de supervisión de la integridad se pueden configurar para grupos de servidores o servidores individuales; de esta forma, se simplificará la implementación y gestión de conjuntos de reglas de supervisión.
- Configuración de la línea base: se pueden establecer perfiles de seguridad de línea base y usarlos para comparar cambios con el propósito de activar alertas o determinar las acciones adecuadas.
- Supervisión práctica y flexible: el módulo de supervisión de la integridad ofrece flexibilidad y control para optimizar las actividades de supervisión en un entorno único. Entre ellas, encontramos la capacidad para incluir/excluir archivos o nombres de archivo comodín e incluir/excluir subdirectorios en los parámetros de exploración. También reporta la flexibilidad necesaria para crear reglas personalizadas de acuerdo a requisitos exclusivos.

## **INSPECCIÓN DE REGISTROS**

### ***Búsqueda y aprendizaje de los eventos de seguridad escondidos en archivos de registro***

El módulo de software de inspección de registros de Deep Security ofrece la posibilidad de recopilar y analizar los sistemas operativos y registros de aplicaciones en busca de eventos de seguridad. Las reglas de inspección de registros optimizan la identificación de eventos de seguridad importantes escondidos en múltiples entradas del registro. Dichos eventos se reenvían a un sistema SIEM o al servidor de registro centralizado para realizar tareas de correlación, documentación y archivado. El agente Deep Security Agent también reenviará la información del evento a Deep Security Manager. Entre las ventajas del módulo de inspección de registros se encuentran las siguientes:

- Detección de comportamiento sospechoso: el módulo proporciona visibilidad en los comportamientos sospechosos que pueden estar sucediendo en los servidores.
- Recopilación de eventos de todo el entorno: el módulo de inspección de registros de Deep Security es capaz de recopilar y correlacionar los eventos de las plataformas de Microsoft Windows, Linux y Solaris, los eventos de aplicaciones procedentes de servidores Web, servidores de correo, SSHD, Samba, Microsoft FTP, etc., además de los eventos de registros de aplicaciones personalizados.
- Correlación de eventos distintos: recopila y correlaciona advertencias, errores y eventos informativos de diversa índole, como los mensajes de sistema (disco lleno, errores de comunicación, eventos de servicios, apagado, y actualizaciones del sistema), eventos de aplicaciones (como inicio de sesión/cierre de sesión/errores/bloqueo de una cuenta, errores de aplicación y errores de comunicación) y acciones administrativas (como inicio de sesión/cierre de sesión/errores/bloqueo administrativo y cambios en las políticas o en las cuentas).
- Informes de auditoría para el cumplimiento: se puede generar un registro de auditoría completo de los eventos de seguridad para ayudar a cubrir los requisitos de cumplimiento, como el requisito 10.6 de PCI.

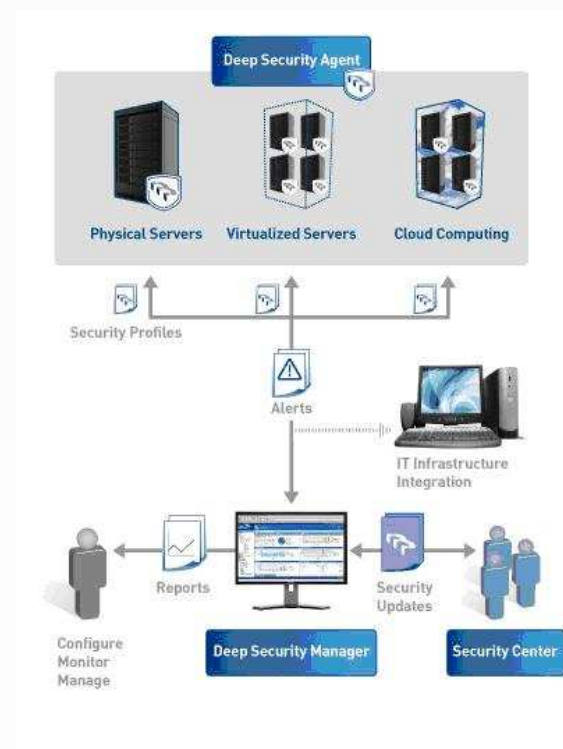
## VI. ARQUITECTURA DE LA SOLUCIÓN DEEP SECURITY

La arquitectura de la solución Deep Security consta de tres elementos:

- Deep Security Agent, que se implementa en el servidor o el equipo virtual que se va a proteger.
- Deep Security Manager, que permite gestionar las políticas de forma centralizada, distribuir las actualizaciones de seguridad y supervisar mediante alertas e informes.
- Centro de seguridad, un portal alojado en el que un equipo de investigación de vulnerabilidades dedicado desarrolla actualizaciones de reglas para las últimas amenazas (actualizaciones que Deep Security Manager implementa).

### MODO DE FUNCIONAMIENTO

El agente Deep Security Agent recibe una configuración de seguridad (por lo general, un perfil de seguridad) de Deep Security Manager. Esta configuración de seguridad contiene las reglas de inspección profunda de paquetes, cortafuegos, supervisión de la integridad e inspección de registros que se han aplicado en el servidor. Las reglas que se van a asignar a un servidor se pueden establecer de forma muy sencilla: solo se necesita realizar una exploración de recomendación, con la que se explora el servidor para comprobar el software instalado y se recomiendan las reglas necesarias para protegerlo. Se crean eventos para todas las actividades de supervisión de reglas, eventos que se envían a Deep Security Manager y, de manera opcional, al sistema SIEM. Cualquier comunicación que se establezca entre los agentes Deep Security Agent y Deep Security Manager estará protegida en ambas partes mediante SSL autenticado.



Deep Security Manager realiza un sondeo del Centro de seguridad para averiguar si existe una nueva actualización disponible; si así es, la recupera y la aplica (manual o automáticamente) a los servidores que precisan de la protección adicional que tales actualizaciones proporcionan. Cualquier comunicación que se establezca entre Deep Security Manager y el Centro de seguridad también estará protegida en ambas partes mediante SSL autenticado. Deep Security Manager también se conecta a otros elementos de la infraestructura de TI para simplificar la gestión; así, se puede conectar a VMware vCenter y a directorios como Microsoft Active Directory para obtener la configuración de los servidores e información sobre los distintos grupos. Además, Deep Security Manager cuenta con una API de servicios Web, que sirve para tener acceso a las funciones mediante programación.

Por su parte, el Centro de seguridad supervisa los orígenes tanto públicos como privados de la información sobre vulnerabilidades a fin de proteger los sistemas operativos y las aplicaciones que los clientes utilizan.

## **DEEP SECURITY MANAGER**

La solución Deep Security pone a disposición controles probados y muy prácticos con los que se hace frente a problemas de seguridad difíciles de resolver. La seguridad operativa y que permite acciones proporciona a la organización el conocimiento (y no únicamente la información) acerca de un evento de seguridad. En muchos casos, se trata de informar de “quién, qué, cuándo y dónde” para poder comprender los eventos del modo correcto y, posteriormente, tomar las acciones que correspondan (distintas de las realizadas por el propio control de seguridad). El software de Deep Security Manager se encarga de los requisitos tanto operativos como de seguridad, con características como las siguientes:

- Sistema de gestión centralizada basada en Web: cree y gestione políticas de seguridad y controle las amenazas y acciones preventivas emprendidas en respuesta a éstas desde una interfaz familiar, similar a la de Internet Explorer.
- Informes detallados: una amplia gama de informes detallados informa de los intentos de ataques y recoge un historial fácil de auditar de las configuraciones de la seguridad y los cambios producidos en ésta.
- Exploración de recomendación: sepa qué aplicaciones se ejecutan en los servidores y equipos virtuales y recomiende los filtros que se deben aplicar a estos sistemas para garantizar una correcta protección con el esfuerzo mínimo.
- Clasificación de riesgos: los eventos de seguridad se pueden visualizar en función del valor del activo, así como de la información sobre vulnerabilidades.
- Acceso basado en funciones: permita que varios administradores (cada uno con niveles de permiso distintos) se centren en distintos aspectos del sistema y reciban información pertinente de acuerdo con sus funciones.
- Panel personalizable: deje que los administradores naveguen por la información específica y accedan a ella y que, asimismo, supervisen las amenazas y las acciones realizadas al respecto. Se pueden crear y guardar varias vistas personalizadas.
- Tareas programadas: las tareas cotidianas (como los informes, actualizaciones, copias de seguridad y sincronización de directorios) se pueden programar para que se realicen de manera automática.

## **DEEP SECURITY AGENT**

Deep Security Agent es un componente de software basado en servidor de la solución Deep Security que habilita el sistema IDS/IPS, la protección de las aplicaciones Web, el control de aplicaciones, el cortafuegos, la supervisión de integridad y la inspección de registros. Este agente se encarga de defender el servidor o los equipos virtuales mediante la supervisión del tráfico entrante y saliente en busca de desviaciones de los protocolos, contenido que indique un ataque o infracciones de políticas. Cuando es necesario, Deep Security Agent interviene y neutraliza la amenaza al bloquear el tráfico malicioso.

## **CENTRO DE SEGURIDAD**

El Centro de seguridad, que es parte esencial de la solución Deep Security, se compone de un equipo de expertos en seguridad de gran dinamismo que ayuda a los clientes a anticiparse a las últimas amenazas, para lo cual ofrece una respuesta rápida y a tiempo a innumerables vulnerabilidades y amenazas a medida que van surgiendo, además de un portal para que los clientes tengan acceso a las actualizaciones e información de seguridad. Estos expertos emplean un proceso de respuesta de seis pasos riguroso, a la par que rápido, que complementan con herramientas automatizadas de gran sofisticación:

- **Supervisar:** se supervisan más de 100 orígenes de datos (públicos, privados o gubernamentales) de forma sistemática e ininterrumpida para detectar y correlacionar las nuevas amenazas y vulnerabilidades importantes. El Centro de seguridad aprovecha las relaciones con distintas organizaciones para recabar información avanzada (y, en ocasiones, previa a su publicación) sobre las vulnerabilidades. De este modo, podrá proveer a los clientes de una protección precisa y oportuna. Entre estos orígenes se incluyen Microsoft, Oracle y otras advertencias de proveedor, SANS, CERT, Bugtraq, VulnWatch, PacketStorm y Securiteam.
- **Dar prioridad:** tras la supervisión, se establece una prioridad de las vulnerabilidades para seguir analizándolas, prioridad que se basa en una evaluación del riesgo para los clientes, así como en los acuerdos de nivel de servicio.
- **Analizar:** después se lleva a cabo un análisis profundo de las vulnerabilidades para averiguar cuál es la protección necesaria.
- **Desarrollar y probar:** a continuación, se desarrollan y prueban exhaustivamente los filtros de software que van a proteger las vulnerabilidades y las reglas que recomiendan dichos filtros para, así, minimizar las posibilidades de falsos positivos y asegurarse de que los clientes pueden implementarlos con rapidez y sin ningún tipo de problema.
- **Entregar:** estos nuevos filtros se entregan a los clientes a modo de actualizaciones de seguridad. Cuando se publique una nueva actualización de seguridad, los clientes recibirán un aviso instantáneo a través de una alerta en Deep Security Manager. Los filtros se pueden aplicar manual o automáticamente a los servidores afectados.
- **Comunicar:** la comunicación con los clientes es constante gracias a las advertencias de seguridad, en las que se describen las vulnerabilidades de seguridad recién descubiertas con todo lujo de detalles.

## **LA INVESTIGACIÓN PROACTIVA MEJORA AÚN MÁS LA PROTECCIÓN**

Aparte de todo lo anterior, el equipo del Centro de seguridad realiza investigaciones constantemente para mejorar los mecanismos de protección en general. Esta tarea depende en gran medida de los resultados y tendencias puestos de manifiesto durante el proceso de respuesta a amenazas y vulnerabilidades. Asimismo, estos resultados afectan al modo en que los nuevos filtros y reglas se crean y la calidad de los mecanismos de protección existentes, algo que a la larga mejora la protección general.

## **PROTECCIÓN DE UNA AMPLIA GAMA DE VULNERABILIDADES**

El Centro de seguridad desarrolla y pone a disposición filtros con los que se protegen las aplicaciones comerciales sin personalizar, así como las aplicaciones Web personalizadas. Los filtros de explotación y vulnerabilidad son reactivos en el sentido en que se usan como respuesta a la detección de una vulnerabilidad conocida. Los filtros inteligentes, por el contrario, reportan una protección proactiva. Con los filtros de supervisión de la integridad se comprueban los distintos componentes del sistema y sus propiedades concretas, y avisan al administrador si se cumple una serie de condiciones de activación específica. Algunos de los componentes que se pueden supervisar son los directorios del sistema, los archivos, el registro de Windows, las cuentas de usuario, los puertos y los recursos compartidos de la

red. Mediante los filtros de inspección de registros se analizan los registros del sistema operativo y de las aplicaciones de otros fabricantes, y avisan al administrador cuando tienen lugar unos eventos determinados.

## **PORTAL DEL CENTRO DE SEGURIDAD**

El portal del Centro de seguridad constituye un punto de acceso único y seguro a la información y asistencia relativas a los productos, como, por ejemplo:

- Actualizaciones de seguridad
- Advertencias de seguridad
- Información de puntuación de CVSS de las vulnerabilidades
- Resúmenes de alertas de Microsoft Tuesday
- Búsqueda avanzada de vulnerabilidades
- Plena divulgación de las vulnerabilidades, incluidas aquellas que Third Brigade no protege
- Información de parches de cada vulnerabilidad
- Canales RSS
- Vales de problemas
- Descargas de software
- Documentación del producto

## **VII. IMPLEMENTACIÓN E INTEGRACIÓN**

La solución Deep Security está diseñada para implementarse rápidamente en la empresa. Así, utiliza la infraestructura y las inversiones existentes para integrarse en ellas a fin de ayudar a lograr una mayor eficacia operativa y contribuir a reducir los costes operativos.

- Integración con VMware: la perfecta integración con VMware vCenter y ESX Server permite importar a Deep Security Manager información de carácter organizativo y operativo de los nodos de vCenter y ESX y, asimismo, que se aplique una seguridad pormenorizada en la infraestructura empresarial de VMware.
- Integración con SIEM: los eventos de seguridad de servidor detallados se proporcionan a través de muy diversas opciones de integración con SIEM, como ArcSight, Intellitactics, NetIQ, RSA Envision, Q1Labs, LogLogic y otros sistemas.
- Integración con directorio: se integra con directorios empresariales como Microsoft Active Directory.
- Comunicación de gestión configurable: tanto Deep Security Manager como Deep Security Agent pueden iniciar la comunicación. Así, se reducen o eliminan los cambios de cortafuegos que solían ser necesarios para los sistemas gestionados de forma centralizada.
- Distribución de software: el software de Agent se puede implementar fácilmente mediante mecanismos de distribución de software estándar como Microsoft SMS, Novel Zenworks y Altiris.
- Filtrado optimizado: contiene funciones avanzadas para controlar los medios de transferencia de datos, como la televisión sobre IP (IPTV), para maximizar el rendimiento.

## VIII. DEEP SECURITY MARCA LA DIFERENCIA

La protección para servidores y aplicaciones de Trend Micro afronta todo un reto como son las necesidades de seguridad operativa y de cumplimiento de normativas de los centros de datos dinámicos de hoy día. Ofrecemos protección total, una mejor eficacia operativa, compatibilidad con plataformas superiores y una integración con las inversiones existentes más estrecha. Además, atendemos antes a los requisitos de nuestros clientes. Con las soluciones Deep Security, obtendrá las siguientes ventajas:

- Una protección más profunda que incluye cortafuegos, detección y prevención de intrusiones, cortafuegos para la capa de aplicaciones, supervisión de integridad del sistema y los archivos e inspección de registros. Todo ello, en una única solución.
- Mayor eficacia operativa: al implementarse de forma rápida y generalizada y automatizar muchas de las tareas clave (como la recomendación de la protección adecuada que se debe aplicar a cada servidor), la solución se gestiona de manera más eficaz y con un impacto mínimo en los recursos de TI existentes.
- Compatibilidad con plataformas superiores: ofrece una funcionalidad completa en más plataformas y admite las versiones actuales de dichas plataformas rápidamente, por lo que permite proseguir con la adopción de las plataformas de virtualización y versiones de SO más novedosas sin renunciar a la protección.
- Integración perfecta: como se integra perfectamente con la infraestructura de TI, además de con el directorio y las plataformas de virtualización (y otras inversiones de seguridad de alto nivel, como SIEM), contribuye a garantizar una implementación empresarial eficaz y una flexibilidad de proveedores continuada.

Para obtener más información, puede llamarnos o visitarnos en:

<http://es.trendmicro.com/es/home/enterprise/>

© 2009 Trend Micro, Incorporated. Reservados todos los derechos. Trend Micro y el logotipo en forma de pelota son marcas registradas o marcas comerciales de Trend Micro Incorporated. "Third Brigade," "Deep Security Solutions" y el logotipo de Third Brigade son marcas comerciales de Third Brigade, Inc. y pueden estar registradas en determinadas jurisdicciones. El resto de los nombres de productos o empresas pueden ser marcas comerciales o registradas de sus respectivos propietarios. La información del presente documento puede modificarse sin previo aviso. WP01TBDS\_ProtDynDC\_090218